



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/500,269	02/08/2000	Kevin L. Fox	GCSD-1078 (S1050	2343

7590 04/22/2004

Richard K Warther
Allen Dyer Doppelt Milbrath & Gilchrist PA
255 S Orange Avenue Suite 1401
PO Box 3791
Orlando, FL 32802-3791

EXAMINER

HO, THOMAS M

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 04/22/2004

17

Please find below and/or attached an Office communication concerning this application or proceeding.

pre

Office Action Summary

Application No.

09/500,269

Applicant(s)

FOX ET AL.

Examiner

Thomas M Ho

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 January 2000.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 are pending.
2. For the completeness of the record, Examiner politely requests Applicant also submit the earliest known date of publication regarding the paper "System Vulnerability Analysis with the Network Visualization Tool" as submitted with the declaration under 37 CFR § 1.131.

Response to Arguments

3. In view of applicant's submission of 131 Declaration showing that inventors had conceived and reduced to practice the invention as claimed before November 4th, 1999, the Examiner now bases Shostack et al. WO/ 99/56195 set forth in the rejections of the previous action, on the textually identical art Shostack et al. US patent 6,298,445, filed Apr. 30, 1998.

Applicant further argues with regards to Shostack et al. on page 5, 2nd paragraph, that "Shostack only shows one module for accessing security vulnerabilities of an operating system and the database of security vulnerabilities. It is not directed to using disparate network vulnerability analysis programs."

Shostack et al. (Column 3, lines 10-35) discloses the use of various modules each accessing the database and analyzing a different aspect of the network. Although not explicitly stated that these are separate network vulnerability analysis programs, Examiner contends that in the development of complex software systems, modules within the system may be large software

packages in themselves. Furthermore it is common and well known for programs to make separate calls to other programs to complete different task for the overall system. Calls to these separate stand alone programs are also known as modules in software architecture.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-3, 5-10, 12-18, 20-23, 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al., Smith, and Yemini.

In reference to claim 1:

Shostack et al. (Column 3, lines 6-34) discloses

A method for assessing the security posture of a network comprising the steps of:

- Exporting only the required data from the system database representing the network to each respective network vulnerability analysis program
- Analyzing the network with each network vulnerability analysis program to produce data results from each program;
- Storing the data results from respective network vulnerability analysis programs and the common system model database within a data fact base;

Shostack et al. fails to explicitly disclose the use of an object model database and decision logic that uses fuzzy logic rules.

Smith(column 4, lines 26-48) discloses a method comprising:

- Applying goal oriented fuzzy logic decision rules to the data fact base to determine the security posture of the network, where fuzzy logic rules are applied to a database of information.

The use of fuzzy logic to analyze information is well known method in the art as disclosed in the background art of Smith(column 3, lines 30-33)

“Fuzzy logic...provides a robust mathematical framework for dealing with “real-world” imprecision and nonstatistical uncertainty.”

And (column 3 lines 38-44)

“Fuzzy rule-based systems have proven effective in a number of application areas such as intelligent control and decision support, especially where a system is difficult to characterize and has strict implementation constraints.”

The applicant describes the object model database as such:

“This model uses object oriented(OO) methodology to provide an extensible set of components in a class hierarchy that can be combined to represent a network. The class hierarchy provides a means of defining components with shared common traits, retaining the specifics that distinguished it from other components. In addition to an implicit hierarchical relationship,

object oriented techniques provide a containment mechanism in which an object can contain a reference to any object, including itself. This provides a flexible mechanism for representing any physical or logical entity. Also, object oriented representation lends itself to ready modification and extension and is ideal for an information assurance arena where changes and new technologies arise daily” (Specification, page 13 line 32 – page 14 line 10)

The examiner takes official notice that an object model database, in the spirit of which it is defined by the applicant, is well known in the art as disclosed by Yemini (column 2, lines 8-12). Yemini specifically discloses that representing knowledge about a system to be monitored such as a network topology may be stored in a hierarchical relational or object oriented database.

It would have been obvious to one of ordinary skill in the art at the time of invention to apply Smith’s fuzzy logic analysis to Shostack’s security mechanism with an object model database implementation, given the advantages of fuzzy logic analysis being equipped to handle uncertainty and imprecision, and given the advantage of object oriented databases being able to handle frequent modification and extension.

In reference to claim 2:

The examiner notes, the applicant(spec page 14, lines 20-23) discloses a filter as the following:

“ NVT views each tool as a filter, calling the appropriate method within the filter to perform the desired task, including initializing, running, importing data, and exporting data.”

Shostack et al. (Column 3, lines 6-34) discloses a method comprising the step of exporting only the required data from the system object model database via filters associated with respective network vulnerability programs, where the filters are the modules that each perform a different task as part of an overall integrated system.

In reference to claim 3:

Shostack et al. (Column 3, lines 6-34) discloses an integrated system of programs for assessing vulnerabilities, with each program assessing a different aspect of the network.

In reference to claim 5:

Though Shostack et al. does not explicitly state that the network analysis programs are created through OOP, it would have been obvious to one of ordinary skill in the art at the time of invention to use object oriented programming in the design of the analysis programs given the advantage of sharing common data and separating source code into hierarchies, and its prevalence as the primary programming paradigm in the software community.

Claims 7,14, 22 are rejected for the same reason as claim 1.

In reference to claim 8:

Smith (column 3 lines 54-58) discloses the use of fuzzy logic based on evidential reasoning.

Claims 9,10 are rejected for the same reasons as claims 2,3 respectively.

Claim 12 is rejected for the same reason as claims 5.

Claim 15,16,23 are rejected for the same reasons as claim 8.

Claims 17,18 are rejected for the same reasons as claims 2,3 respectively.

Claim 20 is rejected for the same reasons as claims 5.

Claim 27 is rejected for the same reason as claim 5.

6. Claims 4,11,19, 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al., Smith, Yemini, and Richardson.

In reference to claim 4:

Richardson(figures 2-6) disclose a program encompassing a method in which the network is modeled as a map on a graphical user interface. It would have been obvious to one of ordinary skill in the art at the time of invention to apply Richardson's graphical user interface and model the network as a map in a GUI to allow the network to be viewed, conveniently navigated the software, and configured by the user.

Claims 11,19,25 is rejected for the same reason as claim 4.

In reference to claim 26:

Richardson (column 1, line 62 – column 2 line 16) discloses a data processing system according further comprising a graphical user interface for displaying the security posture of the network. Richardson's GUI denote the status of particular events based on their severity, allowing the entire status of the network to be inspected by a user looking at the color indications.

Conclusion

7. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR 1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the


Art Unit: 2134

organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

April 16th, 2003


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100